ssh

Existe una forma de loguernos en servidores SSH que implica no tener que escibir usuario/contraseña cada vez y que lo hace más segura. Se trata de utilizar una pareja de claves pública/privada de usuario. La idea es que cada usuario genere su propia pareja de claves y coloque su clave pública en el servidor.

Crear una pareja de claves

```
ssh-keygen -b 1024 -t dsa
```

Al finalizar este comando nos crea dentro de la carpeta de usuario, una carpeta llamada .ssh/, que en su interior alberga la clave pública y privada que acabamos de crear, además de los hosts que ya se conectaron con esta equipo.

Si quisiéramos cambiar el passphrase que nos pide al crear la clave tenemos las siguientes opciones:

- Para DSA. ssh-keygen -f id_dsa -p.
- para RSA. ssh-keygen -f id_rsa -p.

Pasar clave pública a el servidor

Permisos de la carpeta .ssh 700 Permisos del archivo authorized 600

1. cat ~/.ssh/id_dsa.pub | ssh pepito@servidor "cat - >>~/.ssh/authorized_keys"
2. scp ~/.ssh/id_dsa.pub pepito@servidor:.ssh/authorized_keys
3. ssh-copy-id -i ~/.ssh/id_dsa.pub pepito@servidor.

Configuración servidor

- PermitRootLogin without-password (o “no”, directament)
- PubkeyAuthentication yes (activem el sistema d'autentificació per claus)
- PasswordAuthentication no (si no es vol usar més el sistema d'autentificació per contrasenyes)
- RSAAuthentication yes (si a més de poder utilitzar l'algoritme DSA volem permetre claus RSA)

- AuthorizedKeysFile %h/.ssh/authorized_keys (indica l'ubicació i nom de l'arxiu authorized_keys)
- Port. Indicamos el número del puerto de escucha del sshd.
- PermitEmptyPasswords. Permite establece conexión ssh sin ninguna contraseña. No recomendado por el creado del programa.
- PrintMotd i Banner.

El primero específica a sshd si debe imprimir el contenido del archivo /etc/motd Mensaje que se mostrará cuando e
El segundo nos da la posibilidad de enviar el contenido de un archivo específicado anter de permitir la conexión.

- AllowUsers o DenyUsers. Ssh puede acceder a una lista para permitir o no el acceso de usuarios. Estos usuario pueden ser aceptados o denegados por defecto.
- ForceCommand
- LoginGraceTime. Es el tiempo que le damos al usuario para que complete el proceso de logueo. Por defecto son 120 segundos, y si ponemos el valor a 0 es tiempo es infinito.
- MaxAuthTries. Específica el número máximo de conexiones permitidas por usuario. Por defecto es 6.
- Match User i Match Host i Match Address
- StrictHostKeyChecking. Esta opción nos permite establecer en el servidor si preguntaremos o no justo la acción anterior de anotar en el archivo del cliente know_hosts la clave pública para futura conexiones. Si la establecemos como no, directamente el servidor incluirá dicha clave sin preguntar al cliente.

Revision #1
Created 29 November 2023 00:40:26 by adminROM
Updated 29 November 2023 00:40:35 by adminROM